2016

A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Sevgi Ozkan Yildirim
Middle East Technical University

Nazife Baykal
Middle East Technical University

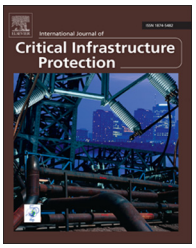
Recommended Citation

Karabacak, B., Ozkan Yildirim, S., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection, 15*, 47-59. https://doi.org/10.1016/j.ijcip.2016.10.001

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness

Bilge Karabacak, Sevgi Ozkan Yildirim, Nazife Baykal*

Graduate School of Informatics, Middle East Technical University, Universiteler Mahallesi, Dumlupinar Bulvari No. 1, 06800 Cankaya, Ankara, Turkey

ARTICLE INFO

Article history:
Received 21 April 2015
Received in revised form
3 October 2016
Accepted 3 October 2016
Available online 5 October 2016

Keywords:
Cyber security
National critical infrastructure protection efforts
Turkey
Developing countries
Maturity model
Grounded theory
Delphi survey

ABSTRACT

Critical infrastructures are vital assets for the public safety, economic welfare and national security of countries. Cyber systems are used extensively to monitor and control critical infrastructures. A number of infrastructures are connected to the Internet via corporate networks. Cyber security is, therefore, an important item of the national security agenda of a country. The intense interest in cyber security has initiated research focusing on national cyber security maturity assessments. However, little, if any, research is dedicated to maturity assessments of national critical infrastructure protection efforts. Instead, the vast majority of studies merely examine diverse national-level security best practices ranging from cyber crime response to privacy protection.

This paper proposes a maturity model for measuring the readiness levels of national critical infrastructure protection efforts. The development of the model involves two steps. The first step analyzes data pertaining to national cyber security projects using grounded theory to extract the root causes of the susceptibility of critical infrastructures to cyber threats. The second step determines the maturity criteria by introducing the root causes to subject-matter experts polled in a Delphi survey. The resulting survey-based maturity model is applied to assess the critical infrastructure protection efforts in Turkey. The results are realistic and intuitively appealing, demonstrating that the maturity model is useful for evaluating the national critical infrastructure protection preparedness of developing countries such as Turkey.

1. Introduction

A physical or cyber infrastructure is designated as a critical infrastructure if its disruption or damage would have a harmful effect on the economy, social order and/or national security of a country [1]. The term critical infrastructure was first used in Executive Order 13010 issued by President Clinton in 1996 [2]. The executive order identified two types of threats against critical infrastructures – physical threats and cyber threats.

Although critical infrastructures have existed long before the widespread use of the Internet and cyber technologies, critical infrastructure protection has become a high governmental priority after the proliferation of cyber systems in

*Corresponding author.
E-mail address: bilgek@alumni.bilkent.edu.tr (B. Karabacak).

http://dx.doi.org/10.1016/j.ijcip.2016.10.001
1874-5482/

infrastructure assets. The cyber systems expose the underlying infrastructures to cyber threats that are asymmetric in nature. A cyber attack has the obvious advantages of anonymity, deniability, affordability and ease of use compared with conventional attacks. Indeed, cyber threats easily and effortlessly pave the way for harmful attacks against critical infrastructure assets. The proliferation of cyber systems has also increased the interdependencies between critical infrastructures. These interdependencies are the main cause of cascading failures that can affect multiple infrastructures [3,4].

Cyber systems, especially SCADA systems and distributed control systems, are widely used to monitor and control critical infrastructures. These industrial control systems are used in power grids, oil and gas pipelines, and water supply and transportation systems. Some critical infrastructure sectors such as finance and telecommunications are completely dependent on, or composed of, conventional cyber systems. Because of new service models such as cloud computing, the networking and Internet infrastructure can be regarded as a component of the critical infrastructure of a country. The 2007 attacks on networks in Estonia demonstrated how much the social and economic well-being of a country is dependent on its Internet infrastructure.

Despite its physically distributed structure, the Internet is logically a single medium. The Internet brings physically distributed people, organizations and nations together. The medium is shared with different types of cyber attackers with different motivations; the attackers range from cyber criminals to state-sponsored entities. A number of critical infrastructures are connected to the Internet over corporate networks [5]. This has led to a number of recorded cyber attacks against critical infrastructures such as nuclear plants, electrical grids, flight control systems and harbors [6,7].

As a result of the increased threats and actual attacks, the cyber resilience of critical infrastructures has become an important requirement of national security. A maturity model that measures its national critical infrastructure protection capability could guide a country in implementing and refining its cyber resilience efforts. However, in the current research literature, there is no study that specifically focuses on a maturity model for national critical infrastructure protection efforts. Some country-level cyber security maturity models have been proposed, but the information about the models and their results is limited. Other studies have been conducted by regional and international organizations. However, these studies focus on scoring and ranking countries according to their national-level cyber security best practices.

This paper addresses the gap in the research literature by proposing a model for measuring the maturity of the critical infrastructure protection efforts of a country. The maturity criteria are determined using a Delphi survey of subject-matter experts. The information provided to the experts before conducting the survey was based on national project data for Turkey. A unique feature of the proposed maturity model is the source of its criteria. Unlike other studies, the maturity criteria are not based on the cyber security best practices of a country, but on the actual cyber posture of the country derived from expert opinion. Another important feature of the survey-based maturity model is that it involved the (unofficial) participation of government officials; other studies that score national efforts generally involve security experts, not government officials. Finally, the proposed maturity model engages a simple maturity formula that incorporates maturity criteria and their weights, and participant assessments of the maturity levels of the country of interest with respect to the criteria.

2. Literature review

This section summarizes and compares six studies related to national cyber security maturity assessment. Cyber security is the main focus of four of the six studies. The remaining two studies consider cyber security as a parameter of national cyber power. Two studies were performed by academic entities whereas four studies were conducted by regional or international organizations, or governments.

The Community Cyber Security Maturity Model (CCSMM) [8], which was developed in a government-funded academic study, assesses holistic cyber security programs at five maturity levels and provides guidance on moving forward to the higher maturity levels. The model checks the existence of various cyber security best practices to determine the maturity level; however, it does not provide a detailed, predefined list of countermeasures corresponding to each maturity level. Moreover, the upper levels of the maturity model are not fully developed because no entity currently has these maturity levels [8]. The model can be adapted to the requirements of different targets – organizations, communities, nations and even individuals. The countermeasures may vary according to the maturity level as well as the type of target. The model has been applied to eleven communities in five U.S. states. However, details of the study are not shared. Additionally, there is currently no national-level application of the model.

The National Cyber Security Maturity Model (NCSecMM) [9] provides guidance to a region or country for measuring its current security status. The National Cyber Security Maturity Model is holistic like the Community Cyber Security Maturity Model [8]. It includes an application framework, roles and responsibilities matrix, implementation guidance and maturity model. It is essentially an adaptation of some of the ISO 27000 standards and CoBIT framework countermeasures to the national context. The National Cyber Security Maturity Model framework includes 34 cyber security processes in five groups. The maturity level of each process is measured individually according to a five-level maturity model adapted from the CoBIT framework. However, the National Cyber Security Maturity Model has not been applied to the national context as yet.

The Cyber Readiness Index was proposed by Melissa Hathaway [10], the former Acting Senior Director for Cyberspace at the U.S. National Security Council. The cyber security efforts of 35 countries have been assessed according to best practices specified by Hathaway using publicly available data from government websites. The maturity levels of the countries are not represented qualitatively or quantitatively and the study concludes that “no country is cyber ready” [10]. Hathaway explains that the goal of the study was “to spark

Table 1 – Summary of maturity models.

Model	Developer	Description	Main theme	Evaluation criteria basis	Data for country evaluations
Community Cyber Security Maturity Model (CCSMM)	University of Texas at San Antonio, USA (Academic Institution)	Holistic maturity model for determining the cyber security postures of organizations, communities and nations	Cyber security	Not specified	Data from government officials
National Cyber Security Maturity Model (NCSecMM)	Mohammad V University at Souissi, Morocco (Academic Institution)	Holistic cyber security model for countries that includes a framework, maturity model, role assignment and implementation guide	Cyber security	ISO 27002 and International Telecommunication Union documents	Country-level evaluation is not performed
Cyber Readiness Index	Hathaway Global Strategies (Private Organization)	Country scoring (35 countries)	Cyber security	Not specified	Data from public sources
Global Cybersecurity Index	International Telecommunication Union (International Agency)	Country scoring and sorting (104 countries)	Cyber security	International Telecommunication Union's Global Cybersecurity Agenda	Data from internal International Telecommunication Union databases, public sources (90 countries) and national stakeholders (14 countries)
Cyber Maturity in the Asia-Pacific Region	Australian Strategic Policy Institute (Non-Governmental Organization)	Country scoring and sorting (18 countries)	Cyber power	Expert opinion	Data from public sources
Cyber Power Index	Booz Allen Hamilton (Private Organization)	Country scoring and sorting (19 countries)	Cyber power	Not specified	Data from public sources, international organizations and The Economist Intelligence Unit

international discussion and inspire global interest in addressing the economic erosion from cyber insecurity that is holding back more robust economic growth."

The Global Cybersecurity Index [11], developed for the International Telecommunication Union (ITU), has been used to assess the cyber security maturity levels of 104 countries. The maturity level of a country is determined based on 17 criteria in five domains derived from the International Telecommunication Union's Global Cybersecurity Agenda [12]. The evaluations were performed using data extracted from internal International Telecommunication Union databases and publicly available resources in 90 countries; only 14 countries provided data specifically for the study. The maturity level of a country is expressed as a normalized value between zero and one. According to the International Telecommunication Union [11], the index has a low level of granularity because it seeks to express the cyber security preparedness of a country and not its detailed vulnerabilities. The 104 countries were ranked from the highest to the lowest maturity levels. There were a total of 29 different maturity levels, meaning that several countries had the same maturity levels.

The Australian Strategic Policy Institute [13] has conducted a cyber maturity analysis of 14 countries in the Asia-Pacific region along with the United Kingdom and United States. The study does not focus solely on cyber security; instead, cyber security is considered to be a dimension of the general cyber maturity of a country. The evaluation criteria and their relative weights were determined with the assistance of experts from government, private sector and academia. The countries were assessed and scored based on publicly available data. The maturity assessment results are presented as percentages and the countries are ranked from the highest to the lowest percentage values.

The Cyber Power Index was created by Booz Allen Hamilton [14] to assess the cyber power of 19 G-20 countries, not including the European Union. Cyber security is not the main focus of the study, but it is, instead, a dimension of the cyber power of a country. The weights of the criteria and the answer choices were determined by a panel of experts. The main sources of data for the evaluations were the International Telecommunication Union, UNESCO, World Bank and The Economist Intelligence Unit.

Table 1 summarizes the six models discussed in the literature along with their attributes. The Community Cyber Security Maturity Model and the National Cyber Security Maturity Model are country-level cyber security maturity assessment models. Four of the models are used to score and sort countries according to their maturity levels. The Cyber Readiness Index and the Global Cybersecurity Index provide country-level scores that are focused on cyber security.

All six models produce maturity evaluations by performing the following two steps in sequence:

1. A set of criteria is specified based on best practices and/or publicly available information sources.
2. A country is evaluated using publicly available data and (sometimes) using questionnaires.

Ideally, maturity model criteria should be grounded on actual country data and vulnerabilities. After creating the maturity model, measurements may be performed by the relevant government officials. These customizations serve to increase the accuracy of the maturity model. The resulting model is of more utility to a country with regard to evaluating its current cyber security posture and the requirements of prospective studies.

These customizations were performed for the maturity model described in this paper. Instead of simply assessing the general national cyber security posture, the resulting maturity model specifically evaluates the critical infrastructure protection efforts of a country. This is of great value because critical infrastructure protection is a common and most vital agenda item in the national cyber security strategies of countries around the world.

3. Motivation, research data and methodology

The basic construct of a maturity model is its maturity criteria. If the criteria are determined by analyzing the actual security posture of a country, then the current situation and progress can be observed more reliably using the maturity model. The first author of this paper was the manager of a state-sponsored project focusing on information security management in critical infrastructures. The project specifically analyzed the cyber dependence of Turkish critical infrastructure assets. The results revealed that the critical infrastructure assets are susceptible to cyber threats because of the inherent vulnerabilities that stem from the use of cyber systems. The authors of this paper analyzed the project data to discover the possible reasons for the susceptibility of the Turkish critical infrastructure to cyber threats. This analysis constituted the first step in developing the proposed maturity model. The second step involved the use of a Delphi survey to determine the criteria based on the root causes of the susceptibility of the Turkish critical infrastructure to cyber threats.

Fig. 1 shows the steps involved in developing the maturity model. The root causes of the susceptibility of critical infrastructures to cyber threats were extracted from project data using grounded theory. Grounded theory is an interpretive, qualitative and inductive data analysis method; fundamentally, it involves the discovery of theory through the analysis of data [15].

In the research, qualitative data was rigorously coded and the codes were categorized during the open coding phase. Categories were compared to find the themes during the axial coding phase. Redundant, trivial and irrelevant themes were eliminated to extract the theory during the selective coding phase.

The project data comprised interview texts and various types of official documents. Data collection and interviews were performed until theoretical saturation; this is the point at which no new data appears and all concepts in the theory are well-developed.

Nine semi-structured interviews were performed. The interviewees were mid-level managers and employees of information processing departments of critical infrastructure

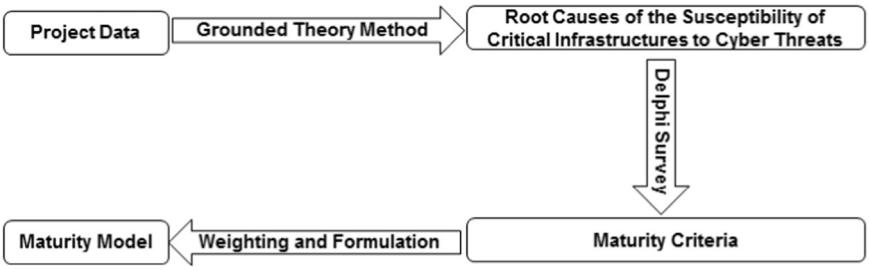


Fig. 1 – Steps in developing the maturity model.

assets. The interviews provided focused, in-depth and rich data of the phenomena under analysis. The interviews involved open-ended questions about the general security posture, threats, potential vulnerabilities, implemented countermeasures and weaknesses of the interviewees' organizations and critical infrastructure sectors. The questions were posed as initiators and catalyzers of the long-lasting and evolving interviews.

A total of 309 documents associated with 91 government or private organizations were collected. Most of the organizations were from the energy, telecommunications, finance, transportation, water management and public services sectors. The documents were categorized into five groups:

- *Meeting minutes*: These corresponded to the notes taken by the researchers during the state-sponsored project.
- *Independent evaluation reports*: These corresponded to the results of information security audits and analyses of critical infrastructure assets performed by independent third parties.
- *Regulation texts*: These corresponded to the laws and statutes that regulate the critical infrastructures considered in the research.
- *Organizational reports*: These corresponded to the documents prepared by the organizations, such as annual activity reports, annual plans and strategic plans.
- *News and media reports*: These corresponded to media excerpts related to the critical infrastructures considered in the research.

Except for the meeting minutes and independent evaluation reports, all the documents listed above were, for the most part, publicly available.

Triangulation using different sources of data was performed to conduct an internal validation of the research [16]. The meeting minutes, independent evaluation reports and news and media reports were considered to be external to the organizations because they were created by third parties. On the other hand, the regulation texts and organizational reports were prepared by the organizations and were, therefore, considered to be internal documents.

The data analysis involved three types of data coding, which were repeated in four iterations. The fourth iteration was the point at which theoretical saturation occurred; at this point, the introduced data does not change the discovered theory [17]. Because grounded theory is a process of theory discovery rather than hypothesis testing, theoretical sampling was performed between the iterations instead of statistical sampling [18]. The researchers reshaped the interview questions, types of sectors and organizations and types of documents based on the theoretical sampling. The results of previous iterations were presented in the semi-structured interviews of the participants during the next iteration to obtain their reactions, such as acceptance, rejection and comments [19].

3.1. *Extracted theory*

The root causes of the susceptibility of critical infrastructures to cyber threats were extracted after four data analysis iterations. A total of ten root causes were identified:

1. Cyber security of critical infrastructures is not perceived by national security authorities as a vital component of national security.
2. Culture of information sharing, collaboration and cooperation within and between critical infrastructure sectors is very limited.
3. Private sector is not perceived by the government and governmental critical infrastructure assets as an important stakeholder in national cyber security efforts.
4. Civil servant and public procurement laws have adverse effects on the cyber security of governmental critical infrastructure assets.
5. The number of qualified cyber security experts is limited.
6. Relationship management practices with product/service providers are inadequate in governmental critical infrastructure assets.
7. Information technology audit mechanisms are very limited or are not implemented in governmental critical infrastructure assets.
8. Managers of governmental critical infrastructure assets do not perceive information security as an area of responsibility.
9. Methodical and formal risk management processes are not conducted for governmental critical infrastructure assets.
10. Security is considered by governmental critical infrastructure assets to be an add-on, not a design construct.

The ten root causes were verified by two cyber security experts. Both the experts had received master's degrees and had more than ten years of professional experience in cyber security. Expert 1 was the main organizer of the Turkish national cyber security exercises; he also played a role in establishing Turkey's National Computer Security Incident

Response Team (CSIRT) and managed the CSIRT for six years. Expert 2 worked on risk analysis projects involving government organizations and critical infrastructure assets; he participated in national-level studies related to the adaptation of international standards to the Turkish context. Both the experts agreed on the final list of root causes with minor changes in the wording of some of the root causes to prevent misunderstanding.

The literature analyzing the cyber security posture of Turkey is quite limited. Academic studies and governmental reports were reviewed to find analysis results that would confirm or refute the root causes. The following paragraphs compare the research findings against the existing literature:

- *Root cause* 1: Several articles in the literature confirm the first root cause. Unlike developed countries, where organizations with national security responsibilities play a central role in cyber defense, the cyber security coordination body of Turkey does not have any national security responsibility [20]. The Turkish National CSIRT website does not display security recommendations or bulletins specific to critical infrastructures [21]. According to Action Item #8 of the National Cyber Security Action Plan, an international cyber security exercise must be organized by the end of May 2014 [22]; however, no exercise has ever been organized. Additionally, the National Cyber Security Action Plan was created for the period 2013 through 2014; it is now obsolete because no new action plan is currently in place. The Cyber Security Council of Turkey was established at the end of 2012 by Cabinet Decision [23]. At the June 2013 meeting of the Cyber Security Council, the critical infrastructure list of Turkey was updated. This decision is in the meeting record, but is not part of a regulation [24]. In fact, the Cyber Security Council has not met for the past 15 months.
- *Root cause* 2: At this time, there are no sector-level CSIRTs or a CSIRT specific to industrial control systems such as the ICS-CERT in the United States, although this was urged in Action Item #4 of the now-obsolete National Cyber Security Action Plan. CSIRTs are important because they share information with other CSIRTs, service providers, law enforcement agencies and other key entities [25]. Successful CSIRT operations depend on collaborative and cooperative activities. The lack of security-specific organizations such as CSIRTs is the primary reason for the lack of information sharing, collaboration and cooperation in Turkey. According to an Organisation for Economic Co-operation and Development (OECD) e-government study [26], only 10–25% of the respondents from central and municipal government entities collaborated with other public sector organizations. According to the same report, nearly 50% of the respondents emphasized that the complexity of regulations prevents collaboration. Meanwhile, the legislative infrastructure has not changed since 2007. According to Senturk et al. [23], it is vital that governmental and privately owned critical infrastructure assets collaborate on critical infrastructure protection efforts, but unfortunately no public–private partnership model is currently active in Turkey.
- *Root cause* 3: The contribution of the private sector to national cyber security efforts is minimal [20]. For example, the Cyber Security Council of Turkey does not have a member who represents the private sector as stated in a Cabinet Decision [27] and Electronic Communications Law amendments [28]. The national cyber security strategy and action plan was prepared by a governmental research agency. The draft document was only shared with the related public organizations as noted on the website of the governmental research agency that prepared the strategy [29]. Only six of the 40 participants in the national cyber security exercise organized in 2011 were private organizations [30]. Among the 30 OECD countries, Turkey was #26 in terms of gross domestic spending on research and development in 2013 [31]; this statistic is an indicator of the limited power of the private sector in Turkey.
- *Root cause* 4: All the interviewees from governmental critical infrastructure assets emphasized the adverse effects of the Civil Servants Law on the quality of employees. All the governmental organization interviewees stated that there were three major problems with the Civil Servants Law. First, it grants job guarantees according to the Article 125 [32]. Second, it does not require evaluations of technical performance. Third, Article 43 does not permit higher salaries to be paid to exceptional employees, resulting in high attrition.
  Three interviewees mentioned the adverse effects of public procurement laws on critical infrastructure protection. Specifically, governmental critical infrastructure assets often cannot purchase needed hardware and software due to conditions imposed by public procurement laws. For example, public procurement laws urge the submission of tenders in almost all instances.
- *Root cause* 5: The Turkish Ministry of Development recently published a report that analyzes the problems related to the country's information society [33]. The report states that the available human resources do not meet the requirements of employers in the information technology sector. Additionally, in an employers' association survey, 58% of the participants stated that the qualified workforce deficit is the most important problem facing the sector [33]. In 2014, an authorized government official claimed that there was no cyber security doctoral program at a Turkish university and only six of Turkey's 196 universities had master's programs in the discipline [34].
- *Root cause* 6: The State Supervisory Council, which works under the charge of the Turkish Presidency, examined the security postures of six governmental critical infrastructure assets in 2013. According to the confidential audit report, the owners of the information systems at the assets were mostly private entities that were granted permission to monitor and control the critical systems [35]. The same report points out problems with the authorization procedures of service provider personnel, security clearance procedures, access management processes and nondisclosure agreements. In summary, critical infrastructure assets do not comply with cyber security principles when procuring services and products from third parties. According to another study [36], which evaluated the results of eight information security management projects in governmental

Table 2 – Maturity criteria determined by the Delphi survey.

Root cause of susceptibility to cyber threats	Maturity criterion (i)	Average weight of maturity criterion (W_i)
Cyber security of critical infrastructures is not perceived by national security authorities as a vital component of national security	1. A critical infrastructure protection program (CIPP) that considers cyber threats exists	2.50
	2. The CIPP is managed by a governmental organization that has national security responsibilities and communicates with national security bodies	2.50
	3. A consultant who provides technical, regulatory and diplomatic cyber security advice to the head of the state exists	1.67
	4. Budget is allocated for critical infrastructure protection efforts	2.50
	5. Government agencies set cyber security regulations and check their application in each critical infrastructure sector	1.83
	6. A CSIRT dedicated to the protection of critical infrastructures exists	2.00
	7. A national cyber security strategy that considers the cyber security of critical infrastructures is a part of the national security strategy	2.17
	8. Nationwide risk analysis and risk management activities that cover all critical sectors and sector-wide risk analysis and risk management activities are performed	2.50
Culture of information sharing, collaboration and cooperation within and between critical infrastructure sectors is very limited	9. A public–private partnership program has been developed and is supported by the government	2.33
	10. Regulations specifying intra- and inter-sector information sharing and cooperation principles exist	2.00
	11. Sector-based CSIRTs with information sharing responsibilities specified in regulations exist	1.50
	12. An internationally recognized national CSIRT that cooperates with other national CSIRTs exists	2.00
	13. A technical infrastructure supporting intra- and inter-sector information sharing needs (e.g., online information sharing portals, statistics dashboards, data collection centers) exists	1.67
	14. A national CSIRT that handles cyber incident warnings related to critical infrastructures exists and it coordinates with the relevant sectoral CSIRTs and critical infrastructure assets when necessary	1.83
Private sector is not perceived by the government and governmental critical infrastructure assets as an important stakeholder in national cyber security efforts	15. Government policies and strategies exist that position the private sector as a key player in national cyber security efforts	2.50
	16. Private sector participates in the development ofnational and sectoral cyber security strategies	2.00
	17. Permanent seat exists for the private sector in national boards such as a cyber security council	1.33
	18. Government leadership in innovation, research and development activities, and identification of priority areas related to cyber security	2.33
	19. Extensive private sector participation in national cyber security exercises	1.50
Civil servant and public procurement laws have adverse effects on the cyber security of governmental critical infrastructure assets	20. Critical reviews and updates of legislation affecting critical infrastructures (especially related to the needs of governmental critical infrastructure assets) are performed	2.50
	21. Amendments to regulations exist regarding the hiring of qualified government officials and contract personnel at higher salaries by governmental critical infrastructure assets	2.50
The number of qualified cyber security experts is limited	22. National capacity building plans and strategies exist	2.50
	23. Critical infrastructure assets give preference to internationally accepted certificate holders in employee recruitment efforts	1.67
	24. Adequate number of qualified cyber security training institutions (private, academic or governmental) exist that support and train critical infrastructure asset personnel	1.83
		2.33

Table 2 (*continued*)

Root cause of susceptibility to cyber threats	Maturity criterion (i)	Average weight of maturity criterion (W_i)
	25. Cyber security and information technology curricula exist at all educational levels, from elementary schools to universities	
	26. Special positions exist for cyber security experts in critical infrastructure assets	1.67
Relationship management practices with product/service providers are inadequate in governmental critical infrastructure assets	27. National and sectoral product and service procurement standards and rules exist for critical infrastructure assets	2.67
	28. Established system for certifying the eligibility of information technology companies that provide services to critical infrastructure assets	2.17
	29. Security standards exist for information technology products used in critical infrastructure assets	1.83
Information technology audit mechanisms are very limited or are not implemented in governmental critical infrastructure assets	30. National and sectoral regulations exist that enforce internal and external audits of critical infrastructure assets	2.67
	31. Regular cyber security audits are performed by regulatory authorities of the various critical infrastructure sectors	3.00
	32. Experienced information technology auditors are employed by the internal audit units of critical infrastructure assets	1.67
	33. Sanctions are imposed by regulatory authorities on critical infrastructure assets for nonconformance	1.83
Managers of governmental critical infrastructure assets do not perceive information security as an area of responsibility	34. Regulations exist that make the top-level management of critical infrastructure assets responsible for cyber security	2.83
Methodical and formal risk management processes are not conducted at governmental critical infrastructure assets	35. Regulations exist that require critical infrastructure assets to conduct cyber security risk management processes	3.00
	36. Critical infrastructure assets adhere to a comprehensive security standard such as ISO 27001	2.17
Security is considered by governmental critical infrastructure assets to be an add-on, not a design construct	37. Regulations exist that impose minimum security countermeasures in critical infrastructure assets	2.50
	38. Regulations exist that set the properties of information systems and security countermeasures in critical infrastructure assets	2.33
	39. Sector-specific technical guidance documents exist for the secure design, set-up and operation of computer networks in critical infrastructure assets	1.50
	40. National and sectoral standards exist that specify security best practices for critical infrastructure assets	1.83

organizations, managers in governmental organizations and heads of information technology departments may fallaciously believe that "information security management can and should be achieved by consulting firms" [36].

- *Root cause* 7: A report by the State Supervisory Council [34] emphasizes the lack of internal audit procedures and processes; in particular, some critical infrastructure assets do not even have internal audit units. A report on the Turkish national cyber security exercise [30] points out inherent audit problems in the participant organizations. Fourteen critical infrastructure assets from the telecommunications, finance and public services sectors participated in the national cyber security exercise.
- *Root cause* 8: According to an evaluation of the results of information security management projects in eight critical governmental organizations, top-level managers do not see themselves responsible for information security [36]; five of the eight analyzed organizations were critical infrastructure assets. Enterprise-wide information security was delegated to the heads of information technology departments by top-level managers. In another case, standard information security principles were violated [37]. Therefore, information security governance principles are not followed at critical infrastructure assets, meaning that information security is not seen as a part of corporate governance and business strategies [38,39].
- *Root cause* 9: The lack of information security management systems was the first finding of the national cyber security exercise [30]. According to the exercise report, organizations do not perform risk analyses, which are an essential part and the starting point of risk management efforts [40].
- *Root cause* 10: According to the national cyber security exercise report [30], some exercise participants did not consider security as a main design principle during system

Table 3 – Weight values for answer choices.

Answer choice (A_i)	Explanation
0	No action or very limited action
1	Partial action
2	Comprehensive action

design. The same problem was noted in the audit report of the State Supervisory Council [34], which recommends the consideration of security requirements during the design phase.

3.2. Extraction of criteria using a Delphi survey

A Delphi survey of six experts was conducted to determine the maturity criteria associated with the root causes and their weight values. Two experts were from the private sector and had ten and fifteen years of cyber security experience, respectively. Two experts were from a governmental research institute and had five and fourteen years of cyber security experience, respectively. Two experts were from academia; both of them had fifteen years of experience.

The Delphi survey was conducted by sending emails to the six experts separately to ensure their anonymity [41]. Controlled opinion feedback was supplied to the respondents between the phases [42]. The survey involved five iterations. Significant consensus among the experts was achieved after five iterations [43].

The Delphi survey identified 40 maturity criteria. Table 2 shows the maturity criteria for each root cause; their weights are listed in the third column. The weight of each criterion was computed as the arithmetic mean of the individual scores provided by the six experts.

3.3. Maturity model and survey results for Turkey

The following simple linear additive evaluation model is used to compute the maturity level of critical infrastructure protection efforts of a country of interest (as a percentage):

$$\text{Maturity Level} = \frac{\sum_{i=1}^{p}\left(\frac{\sum_{i=1}^{m} W_i \times A_i}{\sum_{i=1}^{m} W_i \times 2} \times 100\right)}{p} \quad (1)$$

where p is the total number of survey participants, m is the total number of maturity criteria or principles ($m=40$ in this work), W_i is the weight of maturity criterion i and A_i is the weight of the selected answer choice for criterion i.

Note that the numerator represents the maturity percentage as evaluated by a single survey participant. The final maturity level is the arithmetic mean of the evaluations of all the survey participants.

The maturity levels are presented as percentage values, which are more flexible and meaningful to government officials compared with Likert scale values. The Cyber Power Index [14] and the Cyber Maturity in Asia-Pacific Region studies [13] also use percentage values to represent maturity levels. The two studies measure the maturity of cyber capabilities of various countries and are intended to be used by policy makers.

Table 4 – Pilot application results for Turkey.

Participants (p)	Individual maturity percentage $\frac{\sum_{i=1}^{m} W_i \times A_i}{\sum_{i=1}^{m} W_i \times 2} \times 100$ (%)	Maturity level (average maturity percentage) $\frac{\sum_{i=1}^{p}\left(\frac{\sum_{i=1}^{m} W_i \times A_i}{\sum_{i=1}^{m} W_i \times 2} \times 100\right)}{p}$ (%)
1	24.01	20.85
2	28.30	
3	14.20	
4	20.03	
5	28.50	
6	21.59	
7	10.99	
8	22.28	
9	21.02	
10	17.61	

The proposed maturity model is called the Vulnerability-Driven National Cyber Security Maturity Model because the maturity criteria are based on the extracted root causes. The model can also be categorized as a survey-based maturity assessment method. The other numerical values used in the national level cyber security maturity evaluation were the values of the answer choices provided by the survey participants. The existence of each criterion (principle) was checked by each survey participant according to the three answer choices based on the Likert scale shown in Table 3. A country received zero points for no action or a very limited action, one point for a partial action and two points for a comprehensive action.

Table 3 was also used to compute the Global Cybersecurity Index [11]. The approach used for computing the Global Cybersecurity Index is most similar to the one used by the proposed maturity model in terms of its content. The Global Cybersecurity Index is the only study that scores countries exclusively according to their cyber security efforts. Therefore, the same evaluation table was selected to facilitate reliable comparisons of the two approaches.

Before conducting the maturity survey, the 40 maturity criteria were converted into questions (W_i, $i=1..40$). For each question W_i, the three choices for the answer A_i were presented under the question based on Table 3.

The maturity survey was performed with ten participants ($p=10$), who worked at governmental organizations or were former government officials. They participated in national cyber security efforts such as the preparation and review of the national strategy, national cyber security exercises and preparation of national-level cyber security statutes. However, the survey results do not officially represent the maturity level of Turkey because the survey was conducted by researchers, not by the government.

A maturity survey would produce the most accurate results if the questions were answered by the relevant government officials. In general, country-level maturity surveys are answered by experts and their answers are based on publicly available data pertaining to the evaluated countries. Publicly available data may be misleading because the real preparedness levels and government intent can only be known by the appropriate government officials.

Table 5 – Mappings of the model criteria.

Maturity theme/maturity criterion	Maturity model						
	Proposed model	CCSMM	NCSecMM	Cyber Readiness Index	Global Cybersecurity Index	Cyber maturity in the A-P region	Cyber Power Index
Cyber security organization and/or coordinator (2, 5)	×		×	×	×	×	×
National CSIRT organization (12, 14)	×	×	×	×	×	×	
Public–private partnerships (9)	×		×	×	×	×	×
International cooperation and/or engagement (12)	×		×	×	×	×	×
Regulations related to cyber security (30, 34, 35, 38)	×		×		×	×	×
Cyber security program, strategy, plan and policy (1, 7)	×		×	×	×	×	×
Information sharing and cooperation (10, 11, 13, 14)	×	×	×	×	×		
Certification, training, promotion of higher education and capacity building (22, 23, 24, 25, 26)	×	×	×	×	×		
Innovation, research and development programs (18)	×		×	×	×		
Audit, performance evaluation, exercises and benchmarking to measure cyber security development (30, 31, 32)	×	×	×		×		
Participation and engagement of the private sector (15, 16, 17, 19)	×		×	×			
Adoption of information security governance procedures by critical infrastructure assets (34)	×		×		×		
Adoption of (internationally approved) standards by critical infrastructure assets (29, 36, 40)	×			×	×		
Risk analysis and management of critical infrastructure assets (35)	×		×				
Critical review of and amendments to existing laws (20, 21)	×			×			
Budget for cyber security and/or national funding for research (4)	×			×			
Critical-infrastructure-focused CSIRT and sector-based CSIRTs (6, 11)	×						
Nationwide and/or sector-wide risk analysis and management processes (8)	×						
National and/or sectoral product and service procurement standards or rules (27, 38)	×						
Sector-specific technical guidance documents for the secure design, set-up and operation of computer networks (39)	×						
Certification scheme for information technology companies eligible to provide information technology services to critical infrastructure assets (28)	×						
Cyber security consultant (cyber czar) to the president or prime minister of a country (3)	×						
Minimum security countermeasures for critical infrastructure assets imposed by regulations (37)	×						
Sanctions imposed by regulatory authorities on critical infrastructure assets for nonconformance (33)	×						
Technical infrastructure for intra- and inter-sector information sharing (13)	×						
Public awareness programs		×	×		×	×	
Situational awareness mechanisms				×			
Rapid reaction mechanisms				×			
Identification of appropriate experts and policymakers in government, private sector and academia			×				
Ability to persuade national leaders			×				

Table 4 shows the results of the maturity survey along with the individual maturity percentages. Specifically, the cyber security maturity of the Turkish critical infrastructure protection efforts is assessed as 20.85%.

It is worth noting that the maturity percentage of Turkey was 64.7% according to the Global Cybersecurity Index computed by the International Telecommunication Union [11]. In fact, Turkey received the seventh highest score among the 29 levels in the study. The considerable difference between the maturity levels of two studies may result from the levels of detail of the analyses. The proposed Vulnerability-Driven National Cyber Security Maturity Model evaluates the organizational structures, CSIRTs, regulatory infrastructure, etc. On the other hand, the Global Cybersecurity Index considers the existence of these entities and features, not their details.

For example, the Global Cybersecurity Index only checks if the national and sectoral CSIRTs are legally mandated and the ability of the national CSIRT to gather its own intelligence. In contrast, the proposed maturity model considers the following detailed criteria for a CSIRT:

- A CSIRT dedicated to the protection of critical infrastructures exists.
- Sector-based CSIRTs with information sharing responsibilities specified in regulations exist.
- An internationally recognized national CSIRT that cooperates with other national CSIRTs exists.
- A technical infrastructure supporting intra- and inter-sector information sharing needs (e.g., online information sharing portals, statistics dashboards, data collection centers) exists.
- A national CSIRT that handles cyber incident warnings related to critical infrastructures exists and it coordinates with the relevant sectoral CSIRTs and critical infrastructure assets when necessary.

The scope of the proposed maturity model is the cyber security posture of national critical infrastructures. However, the scope of the Global Cybersecurity Index is the general cyber security efforts of countries. This could also be a reason for the difference between the results.

Turkey has a Cyber Power Index of 30.4%, ranking it #15 among the nineteen countries evaluated [14]. This percentage value is close to the value of 20.85% obtained using the proposed model. However, the theme of the Cyber Power Index is broader than cyber security. In fact, there are four categories in the Cyber Power Index. The criteria related to cyber security – as well as some other criteria that are not related to cyber security – come under the legal and regulatory framework category. The maturity level of Turkey is 49.2% for this category. However, the ranking of Turkey for this category does not change despite its relatively higher maturity. Again, differences in the details of the two models may be the reason for the difference in the maturity percentages. The criteria (principles) underlying the Cyber Power Index are also not as well detailed as for the Global Cybersecurity Index. Additionally, other criteria included in the legal and regulatory framework, such as intellectual property protection, may be a reason for the relatively high maturity level.

Although the proposed maturity model is based on data specific to Turkey, it can produce useful results for countries that are similar to Turkey in terms of organizational and legislative characteristics. However, before conducting a survey for another country, the weight values of the criteria should be reviewed and modified appropriately by experts from the country of interest.

4. Comparison with other models

Maturity models are compared in terms of their maturity criteria. In order to perform comparisons, similar criteria must be generalized to produce a maturity theme.

Table 5 presents the maturity themes and criteria that are related to critical infrastructure protection and incorporated in at least one maturity model. The numbers in parentheses in the first column of Table 5 are the sequence numbers of the relevant criteria of the proposed maturity model. Table 2 lists the criteria underlying the proposed maturity model along with their sequence numbers.

The proposed maturity model provides multiple, thorough criteria for CSIRT organization, national level organization, capacity building, cyber security legislation, and audit and risk management. The first ten criteria are commonly used in other maturity models as well as in the proposed maturity model. The next six criteria are less commonly used in other maturity models. The following nine criteria are unique to the proposed maturity model. The next five criteria are not included in the proposed model, although they are included in other maturity models. Public awareness is a commonly used criterion, but it is not considered in the proposed maturity model. The reason is that the proposed model is specifically designed to evaluate governmental critical infrastructure protection efforts.

5. Conclusions

This paper has proposed the Vulnerability-Driven National Cyber Security Maturity Model for measuring the readiness levels of national critical infrastructure protection efforts. The model is the first academic effort to measure the maturity level of country-level efforts related to critical infrastructure protection. Although the maturity model is based on data specific to Turkey, it can produce accurate results for countries that are similar to Turkey with regard to cyber security studies, technical infrastructure and the legislative environment. However, before conducting a survey, the weights of the maturity criteria must be reviewed and adjusted by individuals with strong expertise related to the countries being assessed.

The root causes extracted from the available data using grounded theory are limited by the opinions of interviewees, collected documents and the theoretical sensitivity of the researchers. The maturity criteria and their weights are dependent on the opinions of the experts participating in the Delphi survey. The maturity percentage of Turkey calculated in this work is dependent on the answers provided by the participating government officials. However, the

calculated maturity level is unofficial because the survey was conducted as part of a government-funded research project, not as an official Turkish government study.

The proposed maturity model is specifically designed to assess the maturity of national critical infrastructure protection efforts. Domains such as combating cyber crime, military cyber operations and privacy protection are not directly associated with critical infrastructure protection [44]. Therefore, these domains are outside the scope of this research and the proposed maturity model. Likewise, the vulnerabilities associated with the physical security of critical infrastructure assets are out of scope. In fact, the criteria related to these domains are excluded from the comparison table (Table 5).

Future research will attempt to extract and model dependencies between the root causes with the goal of devising a maturity model that takes the dependencies into account. Indeed, key dependencies exist among the root causes. For example, the number of qualified cyber security experts in a country depends on the perceptions of cyber security by the government and the private sector.

Acknowledgments

The authors wish to thank to Dr. Soner Yildirim (METU) for his advice regarding the selection of the data analysis method and his assistance throughout the exhaustive data analysis process. The authors also wish to thank Dr. Erhan Eren (METU) for his ideas that initiated the development of the maturity model. This research was funded by the Turkish Ministry of Development under Grant no. 2012K120110 and used data from the Information Security Management of Critical Infrastructures Project.

REFERENCES

[1] ABI Research, Global Cybersecurity Index: Conceptual Framework, London, United Kingdom, 2014.
[2] Booz Allen Hamilton, Cyber Power Index: Findings and Methodology, McLean, Virginia, 2011.
[3] A. Chan, E. Yung, P. Lam, C. Tam and S. Cheung, Application of Delphi method in selection of procurement systems for construction projects, *Construction Management and Economics*, vol. 19(7), pp. 699–718, 2001.
[4] P. Cichonski, T. Millar, T. Grance and K. Scarfone, Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, Special Publication 800-61, Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, 2012.
[5] W. Clinton, Executive Order 13010 – Critical Infrastructure Protection, The White House, Washington, DC, 1996.
[6] S. Condron, Getting it right: Protecting American critical infrastructure in cyberspace, *Harvard Journal of Law and Technology*, vol. 20(2), pp. 403–422, 2007.
[7] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Thousand Oaks, California, 2008.
[8] M. Denscombe, *The Good Research Guide for Small-Scale Social Research Projects*, Open University Press, Maidenhead, United Kingdom, 2010.
[9] M. El Kettani, T. Debbagh, NCSecMM: A national cyber security maturity model for an interoperable national cyber security framework, Proceedings of the Ninth European Conference on e-Government, pp. 236–247, 2009.
[10] I. Eusgeld, C. Nan and S. Dietz, "System-of-systems" approach for interdependent critical infrastructures, *Reliability Engineering and System Safety*, vol. 96(6), pp. 679–686, 2011.
[11] J. Farwell and R. Rohozinski, Stuxnet and the future of cyber war, *Survival*, vol. 53(1), pp. 23–40, 2011.
[12] T. Feakin, J. Woodall and K. Aiken, Cyber Maturity in the Asia-Pacific Region 2014, Australian Strategic Policy Institute, Barton, Australia, 2014.
[13] M. Hathaway, Cyber Readiness Index 1.0, Hathaway Global Strategies, Great Falls, Virginia, 2013.
[14] C. Hsu and B. Sandford, The Delphi technique: Making sense of consensus, *Practical Assessment, Research and Evaluation*, vol. 12(10), 2007.
[15] V. Igure, S. Laughter and R. Williams, Security issues in SCADA networks, *Computers and Security*, vol. 25(7), pp. 498–506, 2006.
[16] G. Ikitemur, Enhancing Cyber Security in Turkey Through Effective Public and Private Cooperation, Ph.D. Dissertation, Department of Public Affairs, University of Texas at Dallas, Richardson, Texas, 2014.
[17] Information and Communications Technology Authority (BTK) and Scientific and Technological Research Council of Turkey (TUBITAK), National Cyber Security Exercise 2011, Final Report, Ankara, Turkey, 2011.
[18] International Telecommunication Union, Global Cybersecurity Agenda, Geneva, Switzerland, 2007.
[19] B. Kaplan and D. Duchon, Combining qualitative and quantitative methods in information systems: A case study, *MIS Quarterly*, vol. 12(4), pp. 571–586, 1988.
[20] B. Karabacak and S. Ozkan, A collaborative process based risk analysis for information security management systems, *Proceedings of the Fifth International Conference on Information Warfare and Security*, pp. 182–192, 2010.
[21] K. Kaska and L. Trinberg, Regulating Cross-Border Dependencies of Critical Information Infrastructure, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2015.
[22] A. Klimburg (Ed.), National Cyber Security Framework Manual, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2012.
[23] R. Little, Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures, *Journal of Urban Technology*, vol. 9(1), pp. 109–123, 2002.
[24] C. Okoli and S. Pawlowski, The Delphi method as a research tool: An example, design considerations and applications, *Information and Management*, vol. 42(1), pp. 15–29, 2004.
[25] Organisation for Economic Co-operation and Development, OECD e-Government Studies: Turkey 2007, Paris, France, 2007.
[26] Organisation for Economic Co-operation and Development, Gross Domestic Spending on R&D 2013, Paris, France (⟨data.oecd.org/rd/gross-domestic-spending-on-r-d.htm⟩), 2013.
[27] Republic of Turkey, Civil Servants Law (in Turkish), Ankara, Turkey, 1965.
[28] Republic of Turkey, Delegated Law about the Organizations and Functions of the Ministry of Family and Social Policies and Law Regarding the Amendments of Certain Laws and Delegated Laws (in Turkish), Ankara, Turkey, 2014.
[29] H. Senturk, Z. Cil and S. Sagiroglu, Cyber security analysis of Turkey, *International Journal of Information Security Science*, vol. 1(4), pp. 112–125, 2012.
[30] R. Shannak and F. Aldhmour, Grounded theory as a methodology for theory generation in information systems research, *European Journal of Economics, Finance and Administration Sciences*, issue no. 15, pp. 32–50, 2009.

[31] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems, Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, Maryland, 2002.
[32] M. Thai, L. Chong and N. Agrawal, Straussian grounded-theory method: An illustration, *The Qualitative Report*, vol. 17 (5), article no. 52, 2012.
[33] Turkish Cabinet, Cabinet Decision on Conducting, Management and Coordination of National Cyber Security Activities (in Turkish), Ankara, Turkey, 2012.
[34] Turkish Computer Emergency Response Team, Cyber Threat List 2015 (in Turkish), Ankara, Turkey, 2015.
[35] Turkish Cyber Security Institute, National Cyber Security Strategy and Action Plan (in Turkish), Ankara, Turkey, 2013.
[36] Turkish General Directorate of Telecommunications, National Cyber Security Activities (in Turkish), Ankara, Turkey, 2014.
[37] Turkish Ministry of Development, The Project for Renewing the Information Society Strategy: Requirements Analysis and Recommendations (in Turkish), Ankara, Turkey, 2013.
[38] Turkish Ministry of Transport, Maritime Affairs and Communications, National Cyber Security Strategy and 2013-2014 Action Plan, Ankara, Turkey, 2013.
[39] Turkish Presidency, Evaluation of National and International Circumstances Regarding Personal Data Protection and Audit Studies Performed in the Context of Information Security and Protection of Personal Data (in Turkish), Ankara, Turkey, 2013.
[40] U.S. Government, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56, Washington, DC, 2001.
[41] R. von Solms and S. von Solms, Information security governance: Due care, *Computers and Security*, vol. 25(7), pp. 494–497, 2006.
[42] S. von Solms and R. von Solms, The 10 deadly sins of information security management, *Computers and Security*, vol. 23(5), pp. 371–376, 2004.
[43] S. von Solms and R. von Solms, From information security to ... business security? *Computers and Security*, vol. 24(4), pp. 271–273, 2005.
[44] G. White, A grassroots cyber security program to protect the nation, *Proceedings of the Forty-Fifth Hawaii International Conference on System Sciences*, pp. 2330–2337, 2012.